Before the

Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
Public Safety and Homeland Security Bureau Makes Available the Recommendations of the Technical Advisory Board for First Responder Interoperability	)))	PS Docket No. 12-74

To: The Commission

COMMENTS OF

NORTHROP GRUMMAN INFORMATION SYSTEMS

Northrop Grumman Information Systems (“Northrop Grumman” [1]) is pleased to provide its comments to the FCC Public Safety and Homeland Security Bureau in response to the Bureau’s May 23, 2012 Public Notice soliciting comment on the recommendations of the Technical Advisory Board for First Responder Interoperability contained in its report, “Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network” (the “Recommendations Report”). Our input is focused on areas where there is an intersection of our corporate experience with the challenges of building and operating the first responder network.

[1] Northrop Grumman Information Systems, a wholly-owned subsidiary of Northrop Grumman Corporation, is a leading provider of IT, systems engineering and systems integration for the Department of Defense, national intelligence, federal civilian and state and local agencies, and commercial customers.

I. Introduction

Northrop Grumman Information Systems (Northrop Grumman) is a wholly-owned subsidiary of Northrop Grumman Corporation. As a leading provider of IT, systems engineering and systems integration, we serve the Department of Defense, national intelligence, Federal civilian and state and local agencies, and commercial customers.

Northrop Grumman is a leader in public safety communications systems; we are one of the world's largest suppliers of 9-1-1 First Responder Computer-Aided Dispatch systems. With a major presence in domestic security initiatives, we are the number one provider of security solutions to the Federal government. Northrop Grumman has deployed next-generation secure broadband wireless networks and interoperable voice communications solutions for defense, intelligence, and public safety agencies across the world.

Our comments cover the following subject areas: 3PP LTE Standards, Interfaces and Guidelines, User Equipment and Device Management, Infrastructure Testing, Priority and Quality of Service, and Security.

II. 3GPP LTE Standards, Interfaces and Guidelines

- Consider adding the following new requirement to Section 4.1.8 (with a conforming reference in the Section 1.3.1 summary): "Hardware and software systems comprising the NPSBN UEs, NPSBN RANs, and Opt-out RANs SHALL operate in the 700 MHz spectrum allocated for public safety broadband (Band 14)."

  Rationale: A requirement should be included for the RF subsystems of the NPSBN to operate in the public safety broadband spectrum (Band 14).

III. User Equipment and Device Management

- To clarify the intent to use "unlocked" devices, consider modifying the proposed requirement #[15] in Section 4.2.1.3 (and modifying the applicable provision in the Section 1.3.2 summary) as follows: "[15] All User Devices (UEs) deployed on the NPSBN that support roaming onto commercial LTE networks SHALL be "unlocked" to support roaming across multiple FirstNet roaming partner networks."

Rationale: The current wording of #[15], which requires a single device to "operate on any FirstNet roaming partner network", sets a difficult standard to achieve in a single device, and is much broader than the descriptive text of Section 4.2.1.3 that recommends "unlocked" UE devices to allow roaming across multiple commercial networks.

IV. Infrastructure Testing

- Consider adding in Section 4.3.4 "Network Application Testing. Provide standards and certification sets for Public Safety trusted applications that regions can use to enable local application control."

Rationale: Even though local control of applications should be possible; there has to be standards and certifications established for Public Safety trusted applications (e.g. NPSTC document on local control in NPSBN[2]) to protect from malware and other risks, especially when connecting to the Internet. The need for local control should be balanced with protecting certified applications equipment and information from attacks due to risks introduced by non-certified applications.

V. Prioritization and Quality of Service

- Consider modifying requirement #[37] in Section 4.7.7 (with a conforming modification to the Section 1.3.6 summary) to remove any implication an industry standard for VPN and MVPN technology exists: "[37] The NPSBN SHALL support the use of openly available VPN and MVPN technology, while providing Priority and Quality of Service for encapsulated applications."

Rationale: The current wording of "the use of industry standard VPN and MVPN technology" could be misinterpreted to suggest there is an industry standard to apply Priority and QOS across VPN and MVPN data streams.

- Consider clarifying and/or limiting the scope of requirement #[30] and consideration #(42) in Section 4.7.2, Section 1.3.6, and Section 1.4.7.

Rationale: The current wording would make it very difficult for the NPSBN to provide predictable and reasonable system performance and service priorities. The prioritized service

[2] Local Control in the Nationwide Public Safety Broadband Network, NPSTC Local Control Task Force Report Rev F. March 2012

should support dynamic changes to reflect current incident status and nature, but must be structured according to a uniform, nationwide set of guidelines and policies. Thus a Priority and QoS framework is required for nationwide interoperability[3].

- Consider adding a new requirement to Section 4.7.4 (with a conforming addition to the Section 1.3.6 summary): "The NPSBN SHALL support assignment of ARP values according to any combination of: user profile (responder function), application service, operating area, and operational state (responder emergency, immediate peril, normal state, etc)."

Rationale: Preemption via ARP level should be assignable by a minimum set of characteristics as described in the referenced NPSTC document, "Priority and QoS in the Nationwide Public Safety Broadband Network." The proposed attributes and mapping to ARP values are required to support prioritization and preemption for responder emergency and immediate peril messages.

VI. Security

- Consider adding a new consideration in Section 4.8.3.1 (and a conforming consideration in the Section 1.3 summary): "Network Access Security. Equipment used in the NPSBN SHOULD support advanced encryption algorithms that are FIPS-140-2 compliant."

Rationale: The cryptographic algorithm recommended in the LTE standard (AES-128 and Snow 3G) are not FIPS-140-2 compliant. The standard provides user device authentication, but does not provide for user authentication. Providing for advanced encryption algorithms and user authentication will enable Federal users to access the NPSBN for their mission needs with commensurate security controls.

- Consider deleting references to Security Assertion Markup Language ("SAML") Section 4.1.11 "Additional Recommended Reference Points and Standards."

Rationale: SAML is one way to implement an Identity Management framework but not the only way. FirstNet should determine a standard approach based on requirements and other architecture factors, when appropriate.

[3] NPSTC "Priority and QoS in the Nationwide Public Safety Broadband Network".Rev 1.0 April 17, 2012

VII. Conclusion

Northrop Grumman applauds FCC's efforts in establishing an industry based Interoperability Board and the Board's efforts in developing these recommendations for an effective deployment of the NPSBN for first responders.

We look forward to working with the FCC, FirstNet and others in the industry to help create a truly secure, interoperable, public safety broadband network that transforms the future operations of first responders and other government agencies.

Respectfully submitted,

NORTHROP GRUMMAN INFORMATION SYSTEMS

Thomas S. Afferton
Director, Public Safety Systems and Solutions

Mark S. Adams
Chief Architect Networks and Communications
Office of the CTO

Northrop Grumman Information Systems
7575 Colshire Drive
McLean, Virginia 22102
(703) 449-3993